

IN THE CLAIMS:

The text of all pending claims (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~striketrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please AMEND claims 14-21 in accordance with the following:

1. (CANCELLED)
2. (PREVIOUSLY PRESENTED) The authentication method as claimed in claim 14, wherein the authentication system authenticates identities of the users prior to supplying a first user with the matching key.
3. (PREVIOUSLY PRESENTED) The authentication method as claimed in claim 14, wherein the authentication system determines whether the prospective transaction is within a previously determined monetary limit.
4. (PREVIOUSLY PRESENTED) The authentication method as claimed in claim 14, wherein the authentication system determines whether the prospective transaction satisfies previously determined conditions.
5. (CANCELLED)
6. (CANCELLED)
7. (PREVIOUSLY PRESENTED) The authentication method as claimed in claim 16, further comprising providing payment of the transaction based on the matching results at the authentication system.
8. (CANCELLED)
9. (CANCELLED)
10. (CANCELLED)
11. (CANCELLED)

12. (CANCELLED)

13. (CANCELLED)

14. (CURRENTLY AMENDED) An authentication method for authenticating users having respective terminal devices and users who are parties to a transaction, comprising:

checking, at an authentication system in response to accesses to the authentication system from terminal devices of the users, whether each of the users satisfies conditions for conducting a prospective transaction;

~~selecting identical transaction keys on screens of the terminal devices; transmitting respective, different matching keys from the authentication system to the terminal devices. If identical transaction keys are selected on screens of the terminal devices and if each of the users satisfies the conditions, said different matching keys being generated based on the identical transaction keys;~~

generating different matching keys based on the identical transaction keys;

transmitting the respective different matching keys from the authentication system to the terminal devices;

inputting, into a given one of the terminal devices, one of the matching keys that has been transmitted to and received by another one of the terminal devices;

transmitting said one of the matching keys from said given one of the terminal devices to the authentication system;

checking, at the authentication system, whether said one of the matching keys matches one of the transmitted matching keys; and

notifying said one of the terminal devices a result of the checking of the matching keys.

15. (CURRENTLY AMENDED) An authentication system for authenticating users who are parties to a transaction, comprising:

a first unit checking, in response to an access to the authentication system from terminal devices of the users, whether each of the users satisfies conditions for conducting a prospective transaction;

a second unit transmitting respective, different matching keys to the terminal devices after if identical transaction keys are selected on screens of the terminal devices, ~~and if each of the users selecting the identical transaction keys satisfies the conditions~~, said different matching keys being generated based on the identical transaction keys;

a third unit receiving, from a given one of the terminal devices, one of the matching keys that has been transmitted to and received by another one of the terminal devices and then passed to said given

one of the terminal devices; and

a fourth unit checking whether said one of the matching keys matches one of the matching keys transmitted from the authentication system.

16. (CURRENTLY AMENDED) A user apparatus for authenticating one of users who are parties to a transaction via an authentication system, wherein the authentication system checks, in response to accesses to the authentication system from respective user apparatuses of the users, whether each of the users satisfies conditions for conducting a prospective transaction, said user apparatus comprising:

a first unit transmitting a transaction key, selected on a screen of the user apparatus, to the authentication system, which responds by transmitting respective, different matching keys to the user apparatuses after~~if~~ identical transaction keys are selected on respective screens of the user apparatuses, ~~and, if each of the users satisfies the conditions,~~ said different matching keys being generated based on the identical transaction keys;

a second unit receiving a first one of the matching keys;

a third unit receiving an input indicative of a second one of the matching keys that has been transmitted to and received by another one of the terminal devices;

a fourth unit transmitting said second one of the matching keys to the authentication system; and

a fifth unit receiving a result of a check performed at the authentication system as to whether said second one of the matching keys matches one of the matching keys transmitted from the authentication system.

17. (CURRENTLY AMENDED) A computer-readable medium storing program code for causing a computer to authenticate users who are parties to a transaction, the program code comprising:

a first unit transmitting a transaction key selected on a screen of the user apparatus to an authentication system, which responds by transmitting respective, different matching keys to user apparatuses after~~if~~ identical transaction keys are selected on screens of the user apparatuses, ~~and if each of the users satisfies conditions,~~ said different matching keys being generated based on the identical transaction keys;

a second unit receiving a first one of the matching keys;

a third unit receiving an input indicative of a second one of the matching keys that has been transmitted to and received by another one of the terminal devices;

a fourth unit transmitting said second one of the matching keys to the authentication system;
and

a fifth unit receiving a result of a check performed at the authentication system as to whether said second one of the matching keys matches one of the matching keys transmitted from the authentication system.

18. (CURRENTLY AMENDED) An apparatus comprising a computer-readable medium storing program code readable by a computer for causing the computer to verify users who are parties to a transaction, the program code comprising:

a first unit transmitting a transaction key, selected on a screen of user apparatus, to the authentication system which responds by transmitting respective, different matching keys to the user apparatuses after if identical transaction keys are selected on screens of the user apparatuses, ~~and if each of the users satisfies conditions,~~ said different matching keys being generated based on the identical transaction keys;

a second unit receiving a first one of the matching keys;

a third unit receiving an input indicative of a second one of the matching keys that has been transmitted to and received by another one of the terminal devices;

a fourth unit transmitting said second one of the matching keys to the authentication system;
and

a fifth unit receiving a result of a check performed at the authentication system as to whether said second one of the matching keys matches one of the matching keys transmitted from the authentication system.

19. (CURRENTLY AMENDED) A computer-implemented method for verifying users having respective user apparatuses and who are parties to a transaction, the method comprising:

transmitting a transaction key, selected on a screen of a user apparatus, to an authentication system which responds by transmitting respective, different matching keys to the respective user apparatuses after if identical transaction keys are selected on corresponding screens of the respective user apparatuses, ~~and if each of the users satisfies conditions,~~ said different matching keys being generated based on the identical transaction keys;

receiving a first one of the matching keys;

receiving an input indicative of a second one of the matching keys that has been transmitted to and received by another one of the terminal devices;

transmitting said second one of the matching keys to the authentication system; and
receiving a result of a check performed at the authentication system as to whether said second one of the matching keys matches one of the matching keys transmitted from the authentication system.

20. (CURRENTLY AMENDED) A computer specially configured by reading and executing program code, stored on a computer-readable medium, for causing the computer to verify users who have respective user apparatuses and who are parties to a transaction, the program code comprising:

a first unit transmitting a transaction key, selected on a screen of a user apparatus, to the authentication system which responds by transmitting respective, different matching keys to the user apparatuses after if identical transaction keys are selected on screens of the respective user apparatuses, ~~and if each of the users satisfies conditions~~, said different matching keys being generated based on the identical transaction keys;

a second unit receiving a first one of the matching keys;

a third unit receiving an input indicative of a second one of the matching keys that has been transmitted to and received by another one of the terminal devices;

a fourth unit transmitting said second one of the matching keys to the authentication system;
and

a fifth unit receiving a result of a check performed at the authentication system as to whether said second one of the matching keys matches one of the matching keys transmitted from the authentication system.

21. (CURRENTLY AMENDED) A program stored in a storage and readable by a computer to control the computer to authenticate users having respective terminal devices and who are parties to a transaction, by:

checking an authentication system in response to an access to an authentication system from respective terminal devices of the users, whether each of the users satisfies conditions for conducting a prospective transaction;

selecting identical transaction keys on screens of the terminal devices; ~~transmitting respective, different matching keys from the authentication system to the terminal devices~~ If identical transaction keys are selected on screens of the terminal devices ~~and if each of the users satisfies the conditions~~, said ~~different matching keys being generated based on the identical transaction keys~~;

generating different matching keys based on the identical transaction keys;

transmitting the respective different matching keys from the authentication system to the terminal

devices;

inputting, into a given one of the terminal devices, one of the matching keys that has been transmitted to and received by another one of the terminal devices;

transmitting said one of the matching keys from said given one of the terminal devices to the authentication system;

checking, at the authentication system, whether said one of the matching keys matches one of the transmitted matching keys; and

notifying said one of the terminal devices a result of the checking of the matching keys.